

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>

**DATE(S) ISSUED:**

06/14/2016

**SUBJECT:**

Vulnerability in Microsoft DNS Server Could Allow for Remote Code Execution (MS16-071)

**OVERVIEW:**

A vulnerability has been discovered in Microsoft's Windows Domain Name System (DNS) Server, which could allow for remote code execution. An attacker who successfully exploited this vulnerability could execute arbitrary code in the context of the Local System Account. Depending on the privileges associated with this account, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**THREAT INTELLIGENCE:**

There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEMS AFFECTED:**

- Windows Server 2012, R2, and Server Core Installations

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **Medium**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **Medium**

**Home users: Low**

**TECHNICAL SUMMARY:**

A remote code execution vulnerability was discovered in Windows DNS Server when it fails to properly handle specially crafted DNS requests (CVE-2016-3227). This vulnerability can be exploited if an attacker issues a malicious request to a vulnerable Windows server configured as a DNS server.

Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the Local System Account. Depending on the privileges associated with this account, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Implement logging and monitor logs to ensure that only authorized users are accessing resources and identify any unauthorized modifications or unusual traffic. Store logs for a minimum of 90 days.

**REFERENCES:****Microsoft:**

<https://technet.microsoft.com/en-us/library/security/ms16-071.aspx>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3227>

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>